

FROM THE

RECEIVED

FEB -3 1994

FCC MAIL ROOM

January 11, 1994

Mr. William F. Canton
Acting Secretary
Federal Communications Commission
1919 M Street NW
Washington, DC 20554

RE: CC Docket no. 93-292

Dear Mr. Canton:

I am a telecommunications professional who is responsible for my company's telecommunication systems and I am painfully aware that although I may reduce the risk, no matter how many steps I take to secure my systems, I am still vulnerable to toll fraud. That is why I am so encouraged by the proposed rule making.

PBX owners should not be responsible for 100% of toll fraud if we are not controlling 100% of our destiny. This destiny is ultimately controlled by not only our implementation and proper use of PBX security features but by the information, equipment and services provided by IXC's, LEC's and CPE vendors. The legal obligations of the IXC's, LEC's and CPE vendors should provide the proper incentive to reduce and eliminate all toll fraud.

Current programs offered by some IXC's (Sprint Guard, MCI Detect, and AT & T Netprotect) and insurance companies are too expensive. Monitoring and proper notification by the IXC's must be a part of the basic interexchange service offerings. This should eliminate cases of toll fraud greater than 24 hours.

LEC's must also provide monitoring and proper notification as a part of their basic services offerings. Local lines are as vulnerable to toll fraud. As the line between IXC and LEC becomes fuzzier, monitoring and proper notification by all carriers will be even more applicable.

CPE vendors need to provide telecommunications security as a cost of doing business instead of an opportunity to sell additional products and services. CPE vendors should be required to provide warnings about the risks of toll fraud, and it specifically relates to their equipment and provide solutions to default passwords, which are well known to the criminal community. All login IDs, including those sued by the vendor, should be disclosed at the time of purchase and at installation. All customers passwords should be changed or created at installation

No. of Copies
Listed in Code

Ques

and the customer should receive written assurance that all vendor passwords will meet minimum requirements regarding length, change schedule, and alpha numeric format. CPE vendors should be encouraged to offer security related hardware and software in the price of their systems.

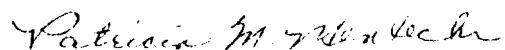
The provisions outlined in the NPRM are fair and equitable. Shared liability will require clearly defining the responsibilities of the;

- CPE owner to secure their equipment
- CPE vendors to warn customers of the specific toll fraud risks associated with their equipment
- IXCs and LECs to offer detection, notification, prevention, and education offerings and services.

If toll fraud occurs due to the negligence of one or more parties then the financial loss should be equitably distributed among those negligent parties. If there is no proven negligence the financial loss should be equitably distributed among CPE owner, and all CPE vendors (s), LEC(s) and IXC(s) involved.

Toll Fraud is a financially devastating problem that effects the entire telecommunications industry including users, vendors and carriers. I am sure, that if we all work together we can and will make a positive impact on this problem.

Sincerely



Patricia M. Mentecki
Telecommunications Specialist

EVERETT S. RICE

SHERIFF

PINELLAS COUNTY, FLORIDA

Pinellas County
Sheriff's Office

Post Office Drawer 2500
Largo, Florida 34649-2500
Telephone (813) 587-6200

January 27, 1994

RECEIVED

FEB - 3 1994

William F. Caton, Acting Secretary
Office of the Secretary
FEDERAL COMMUNICATIONS COMMISSION
ROOM 222
Washington, DC 20554

FCC MAIL ROOM

Re: CC Docket 93-292
In the Matter of Policies
and Rules Concerning Toll Fraud

Dear Secretary Caton:

This letter is intended to serve as the comments of Everett S. Rice, Sheriff of Pinellas County, Florida, an elected constitutional officer of the State of Florida, to the Notice of Proposed Rulemaking (the "Notice") adopted by the Federal Communications Commission ("FCC") on November 10, 1993, and released on December 2, 1993.

BACKGROUND

Pinellas County operates under a Home Rule Charter as adopted by vote of the electorate on October 7, 1980. Pinellas County is the most densely populated county in the State of Florida, with population of nearly 900,000. Two of its twenty-four municipalities are St. Petersburg and Clearwater, which, along with nearly thirty miles of highly regarded beaches, represent significant drawing cards for additional seasonal residents and tourists. As a result, Pinellas County government is quite large, with nearly 3,000 employees.

The geographical layout of the County, in concert with the permanent and evolving demographics, requires an extensive telephone system. The current long distance carrier is American Telephone & Telegraph ("AT&T"), and the telephone hardware and software, and certain maintenance services, are provided by Rolm under a State of Florida contract for the County and the Sheriff. The County and the Sheriff employ telephone experts who work with Rolm on the maintenance services, and on the programming of security codes.

Notwithstanding the efforts of the County and the Sheriff to fully secure their respective telephone systems, both recently have

No. of Copies
1st ANODE

Aug

William F. Caton, Acting Secretary
January 27, 1994
Page 2

been the victims of "hackers." Therefore, both now take the issue of telephone fraud very seriously and very personally, and respectfully request that the FCC make every reasonable effort to protect all of the victims of telephone fraud, including but not limited to residential private line customers, private and public cellular telephone subscribers, small business customers, large business and governmental PBX owners, and the telephone carriers. All of these potential victims represent the County's residents, businesses, and taxpayers.

**GENERAL PROTECTIONS MANDATED
BY GROWING BASE OF VICTIMS**

While the proposed rule change, section 68.200(1), might not serve to relieve the County from its recent "hacking" charges, we believe that the majority of victims deserve enhanced protection. In our case, the victims are not just governmental entities with taxing authority; rather, they are taxpayers ranging from major corporations to retired people on extremely limited fixed incomes. The taxpayers also include a substantial base of small businesses, which are, according to the recent literature on telephone fraud issues, the next prime targets for this fraudulent activity. Given the economy of recent years, they are the entities least capable of surviving a "hacking" episode, and also least capable of preventing it. Mitsubishi may survive a \$900,000 telephone bill, but Fred's Paint Shop could be forced into terminal bankruptcy by a bill of \$9,000. Any relief considered by the FCC must keep all the victims in mind.

We believe there are protections to be considered which may serve to place the financial risks where they most equitably belong. We all recognize that our bills are paid by our taxpayers; any large corporation's or small company's bills are paid by its ultimate customers, and may be paid in the form of reduced stock dividends, perhaps impacting pension funds and the elderly on fixed incomes relying on already modest dividends; any bills not paid by the customer but passed on to the telephone carrier is in fact paid by its customer base. Therefore, as noted below, the regulations need to more clearly and much more equitably, share the risks and damages associated with toll fraud.

Not to be overlooked is the dire need for additional federal legislation imposing harsh penalties for telephone fraud, and where there is any possibility of reimbursement, mandatory restitution sanctions. Such legislative changes could go a long way toward placing the financial burden on the proper parties. The perpetrators, not the victims, must be held accountable for this electronic grand theft.

William F. Caton, Acting Secretary
January 27, 1994
Page 3

COMMENTS

1. PBX Fraud and the Pacific Mutual Petition.

a. The County and the Sheriff emphatically supports the spirit of the Pacific Mutual petition requesting clarification of the tariff provisions, as well as proper allocation "of the costs of remote-access toll fraud among users, carriers, and suppliers, and to promote effective anti-fraud measures." [Text at n.30 of the Notice.] While warnings to customers are meritorious, as proposed by section 68.200(1), they constitute only a partial remedy for the telephone-system-literate customer, and at best an illusory remedy for the average customer, constituting the majority of users in this country. The less sophisticated customer is at the mercy of its own innocence and ignorance, and may be at the mercy of certain un reputable vendors. If disclosure is the FCC's only adopted remedy, please, at least require that it be in a form and be presented in a manner that is proportionate to the level of specific customer sophistication.

b. The points raised by Bell Atlantic in paragraph 13 of the Notice are undeniable: deregulation did remove CPE from the umbrella of the Commission. However, we contend that what was done can be undone. The current situation fosters finger-pointing, and fails to responsibly and decisively allocate responsibility. Mere selection and ownership of the CPE and its features by a customer relying on the representations of manufacturers and vendors is not a proper standard by which to assign liability for the costs of toll fraud.

c. While we are in agreement that the customer should take security steps commensurate with its understanding of the telephone system and the risks of telephone fraud, certain security measures are beyond the economic means of some customers. Call blocking, at a cost of \$5.50 per line per month, would cost the County alone more than \$10,000 a year. The County may, in absolute dollars, be able to afford such a protection, but now has an extremely difficult time justifying such expense to taxpayers. If all goes well in a year, the County has absolutely nothing to show the taxpayers for that expenditure. Small businesses, in some cases, simply could not afford another \$5.50 per month per line, in the face of rising workers compensation and unemployment compensation costs, possible mandatory health care expenses, possible increased minimum wages, and simple inflation impacting businesses daily. Furthermore, more sophisticate real-time monitoring equipment, which the County may well purchase to the tune of \$40,000, is simply out of the reach of most customers. Therefore, we recommend that such additional telephone security costs as may be regulated by the FCC and the State utility agencies be examined and adjusted to reflect the real cost to the carriers, plus some

reasonable profit.

d. We agree that "tariff liability provisions that fail to recognize an obligation by the carrier to warn customers of risks of using carrier services are unreasonable." [Paragraph 24 of Notice.] The proposed text of section 68.200(1) approaches a remedy but falls short of addressing the requisite level of warning as discussed above. It also fails to address the issue of liability when a warning is issued to a customer who is technologically incapable of understanding the ramifications, until that first "hacking" bill arrives. Furthermore, the last sentence of the proposed rule places the customer in an untenable position. That sentence states that a customer's failure to reset default codes may result in great financial exposure. Contrast that with the ruling in Chartways or in American Telephone and Telegraph Co. v. Jiffy Lube International, Inc., 813 F. Supp. 1164 (D. Md. 1993), which would seem to assign full liability to any company which does handle its own security, including setting default codes. We propose that this potential inconsistency be resolved.

e. Issues raised in Paragraph 25 of the Notice:

1) "[W]hat other factors could or should be considered when liability determinations must be made." We agree that the best rule of thumb is that among the "carriers, CPE owners, equipment manufacturers," or others, those "in the best position to avoid, detect, warn of, or control the fraud" should shoulder the liability. Unfortunately, whatever legal theory may apply, in most instances it is not reasonable to assign full responsibility to any one party. A CPE owner may install the best security equipment available, but a dedicated hacker could break in nonetheless. The carrier may be in the best position to identify highly unusual activity on a customer's line, and should be required to under the ultimate regulations. However, moderately unusual activity could signal moderate hacking, or could signal an extremely busy surge in work; the carrier cannot be expected to note every anomaly in telephone activity. The vendors and manufacturers should be required to close as many doors in their systems as possible, and the companies installing and interfacing systems should bear responsibility for not creating new doors, and closing any known doors, including such doors as are reasonably known in the industry. In short, we believe a strictly proportionate liability is the most fair and most realistic; joint and several liability would not be appropriate. There should be a relationship between liability, knowledge of the equipment and the risks, and the ability to avoid the liability.

2) We also agree that "shared liability would require definition of the specific responsibilities of the CPE-owner to secure the equipment or communications system, of the manufacturer

William F. Caton, Acting Secretary
January 27, 1994
Page 5

to warn of toll fraud risks associated with the features of the CPE, and of the carrier to offer detection and prevention programs and education services." Again, the proper approach would be to include great specificity, recognize that technologically the CPE-owner may not be able to comply with certain security directives, and it would be better to require a manufacturer to develop the most secure system as is reasonable. While we would laud continued detection and prevention programs from the carriers, and education services from carriers and the manufacturers, the price should be required to be within the means of the average customer.

3) You seek comment on "what constitutes a failure to meet these responsibilities." As a threshold, the failure to comply with minimal and affordable security measures available to the CPE-owner, failure of the carrier to report unusual activity in excess of an established percentage or of a particular nature (e.g. calls to India on the lines of a small catering company), or the failure to fully and clearly disclose the risks by the manufacturer are among the types of breaches which might realign the liability ratios. Beyond certain obvious considerations, there should perhaps be an opportunity in the appropriate forum to establish mitigating or exacerbating circumstances in defense.

4) You also seek comment on the "nature of damages to be awarded to aggrieved parties." First, full and timely restitution from the perpetrators is the most meaningful type of damage, if it is recoverable. Second, restitution to the other victims from the victim who breached a minimum duty of care, in the form of remaining liable for any damages resulting from any unrepaid hacking. Finally, an adjustment of relative percentage of exposure among the customer, carrier, vendor, manufacturer, or others, as appropriate.

5) You additionally seek comment on the "appropriate forum to resolve these issues." We recommend that a committee appointed for various regions of the country consisting of representatives from customers, carriers, manufacturers, vendors and related industries act as an initial arbitration and/or mediation body. If they are to act only as an advisory board, then the next step should be to the Commission who would best proceed expeditiously with a formal complaint proceeding.

6) If inadequate restitution is forthcoming, then we suggest that the expense of arbitration should be borne in proportion to the final liability for the fraud. If restitution is ultimately available, the perpetrator should also pay this expense.

7) We recommend insulating residential ratepayers from the additional burden of the business fraud. Rather, all like-kind business telephones should bear the higher rates legitimately

William F. Caton, Acting Secretary
January 27, 1994
Page 6

passed on to the carriers by shared liability. In other words, PBX users should bear the industry risk, but the small "meat-and-potatoes", two-line small business telephone service which faces little to no telephone fraud risk because of the simplicity of the system, should not bear the risk of the larger companies using more vulnerable equipment.

f. Issues raised in Paragraph 26 of the Notice:

1) All businesses should be expected to take reasonable and affordable fraud prevention measures commensurate with the sophistication and vulnerability of their telephone systems. The County and the Sheriff have had independent security audits of their respective systems, and have taken steps to comply with the ten-step plan to tighten security. However, some businesses, for instance, cannot do away with remote access communication, and the manufacturers and the carriers must be part of this security loop as their respective costs of doing business. Where affordable by individual government or business, security equipment, such as the call data recorder ("CDR") with a fraud alert feature ordered by the County, is a valuable means of protection; however it is not going to be reasonable to expect smaller governments or businesses to invest in such equipment. In short, improved economy, improved technology, and enhanced law enforcement, rather than mandating an absolute list of fraud prevention devices, is far more beneficial to the homogeneous pool of potential fraud victims.

2) With respect to whether IXC's and LCE's to offer customers protection through monitoring services, all carriers should be required to explain in detail the monitoring services they provide. As a practical matter, the new or expending customer has no knowledge of the tariff requirements, and they should be voluntarily explained by the carrier. In fact, Pinellas County only recently became aware of the monitoring services of AT&T and MCI through publications they receive, to which medium to small governments and businesses are unlikely to subscribe. With respect to whether monitoring services should be offered as part of basic interchange service, we suggest that it should be available as an extra feature, but at a reasonable and affordable price to encourage protection for all potential victims.

3) The availability of security devices is dependent upon the type of system at issue. While we recommend the usage of affordable devices, economy, again, is a real issue of which the Commission should be mindful. CDR's with fraud alert in real time printout and alarming are beneficial but too expensive for medium to smaller governments and businesses. Full toll blocking by the carrier is also outside of the means of many medium to smaller governments and businesses. There are some software toll blocking options available, but they can be bypassed by a knowledgeable

William F. Caton, Acting Secretary
January 27, 1994
Page 7

hacker. Perhaps the best remedy on an ongoing basis is continual auditing of the system for any inadvertent errors in programming, but these too are limited to the larger governments and businesses with deeper expertise on staff or larger budgets. Sometimes one has to spend money to save money, but most telephone customers simply do not have to money to spend to acquire the cadillac of fraud prevention. This principle should be kept in mind in the adoption of any regulations.

4) With respect to general comments pertaining to ultimate liability determination, the County and the Sheriff suggests the following rule of thumb in determining relative liability for fraudulent telephone fraud bills: (a) If a customer has been properly and fully notified of a potential vulnerability, or has been notified of an active breach of the system, and no preventative measures are implemented, the customer should be principally or even fully liable; (b) If a customer has been properly and fully notified of a potential vulnerability, or has been notified of an active breach of the system, and measures are taken to prevent further fraud, then the liability should be shared; (c) If a customer has been properly and fully notified of a potential vulnerability, or has been notified of an active breach of the system, and do not timely prevent a further breach, or cannot do so without vendor assistance or because of honest ignorance, then the apportioned liability should be negotiated.

g. We endorse the Florida rule position explained in note 42, pages 15 and 16 of the Notice, prohibiting a company which provides interexchange services or local exchange services from collecting from the pay telephone provider for charges billed to a line for calls originating from the listed access calls or through an operator. The balance of the Florida PSC position, as represented in that note 42 is also endorsed.

2. Cellular Fraud.

a. It is recommended that each owner of a cellular telephone be assigned a secure Personal Identification Number (PIN) which would be required to be entered prior to the number called, or after the number called, before a charge from the call will be

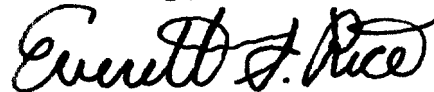
William F. Caton, Acting Secretary
January 27, 1994
Page 8

allowed. This would prevent a stolen telephone to be used without the additional security level of the PIN entry. If the customer is found to be at fault for providing the PIN, such as writing it on the telephone, then the customer is liable for the charges.

b. The problem of "cloning" a telephone's personal system is one beyond the control of the subscriber. Sole liability for this should be assigned to the carrier or the manufacturer, or apportioned between them as responsibility seems to lie.

We appreciate the opportunity to respond to your Notice. If you have any questions concerning this, please feel free to contact the undersigned.

Sincerely,

A handwritten signature in cursive script, reading "Everett S. Rice".

EVERETT S. RICE
Sheriff, Pinellas County
Florida

cc: Fred E. Marquis, County Administrator
Nancy Reppert, Director Risk Management
The Honorable Robert Graham
The Honorable Connie Mack